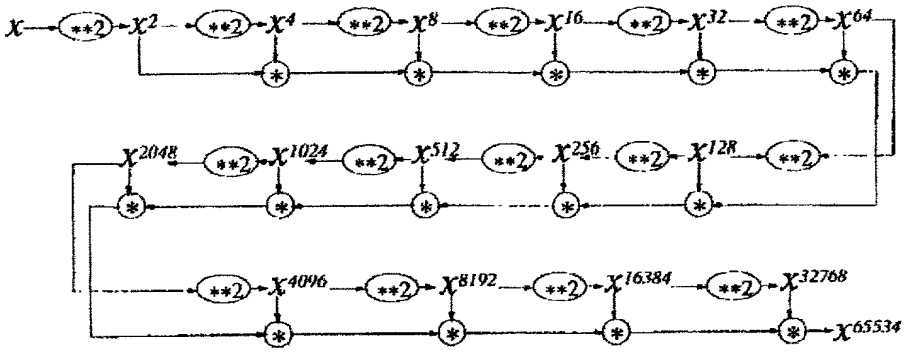
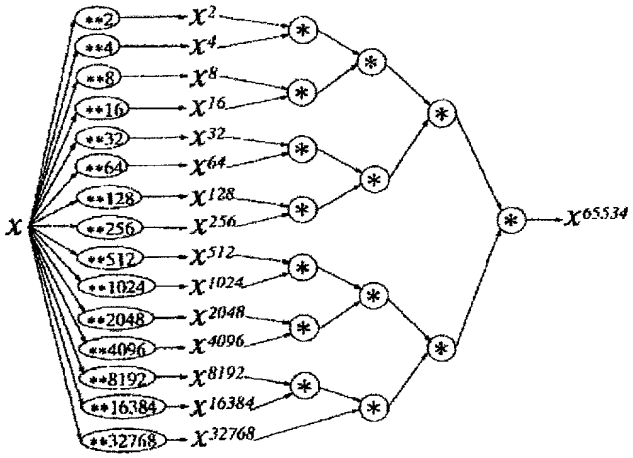


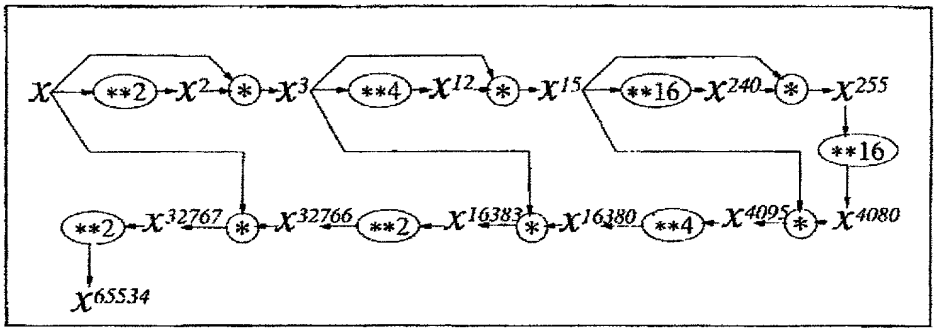
Example calculation process using Fermat's little theorem (m = 16)

Fig. 1



Example calculation process using Fermat's little theorem (m = 16)

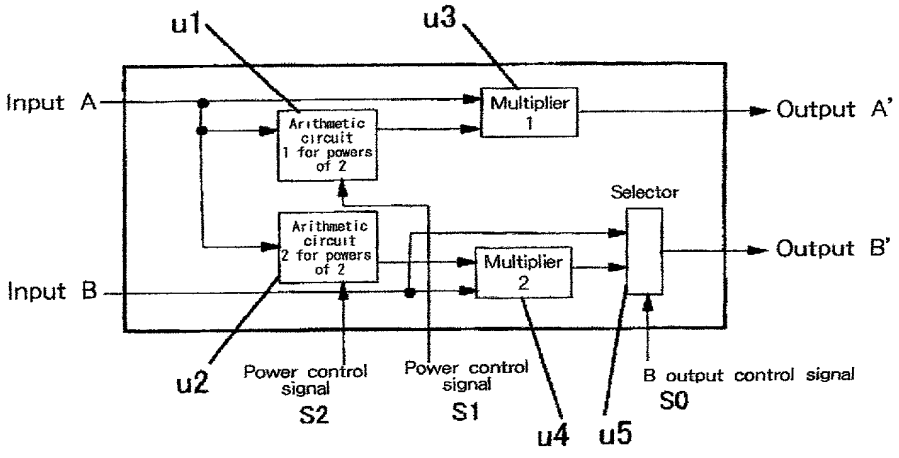
Fig. 2



Example calculation process using the algorithm of Itoh and Tsujii (m = 16)

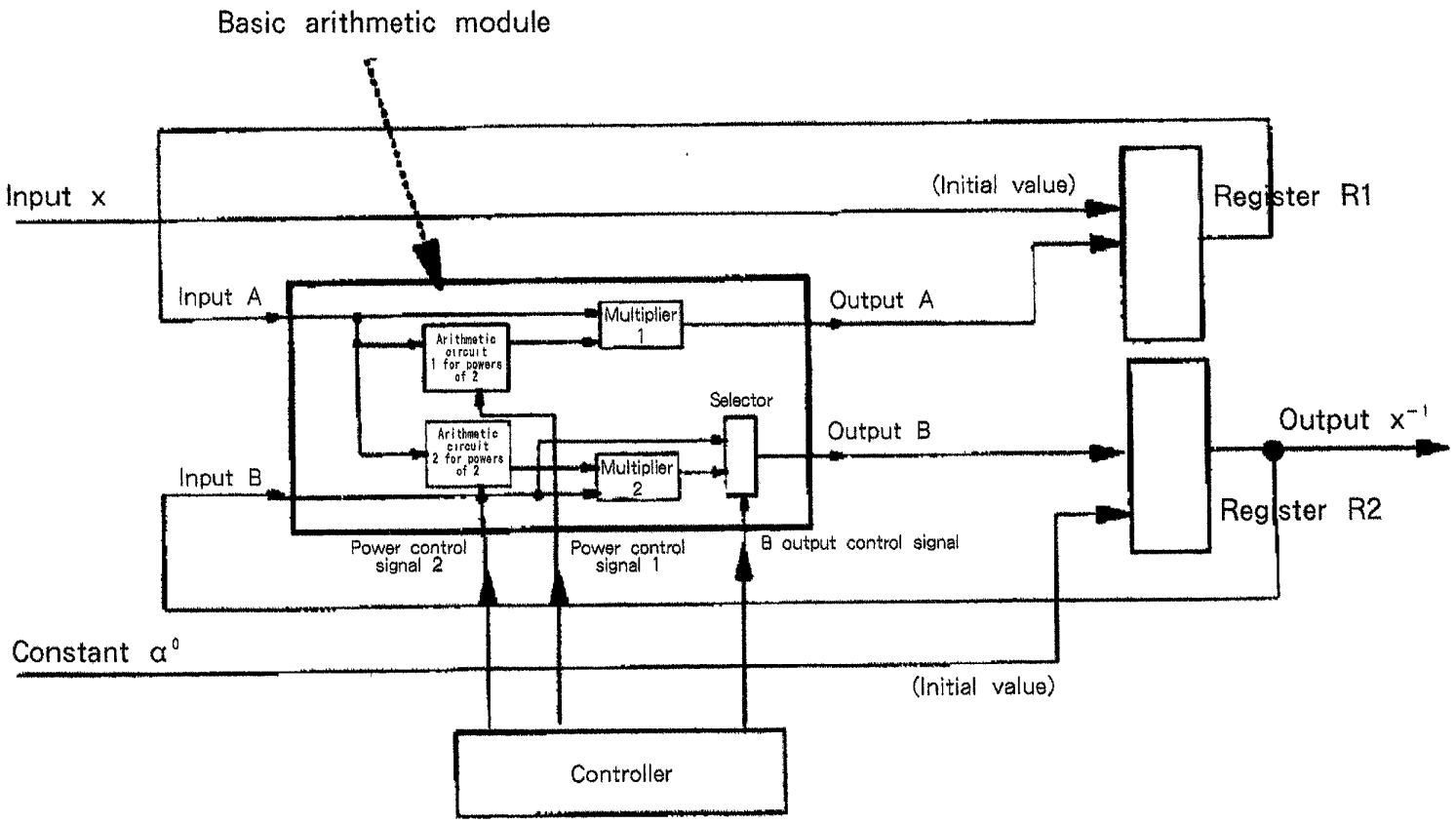
Fig. 3

Basic arithmetic module



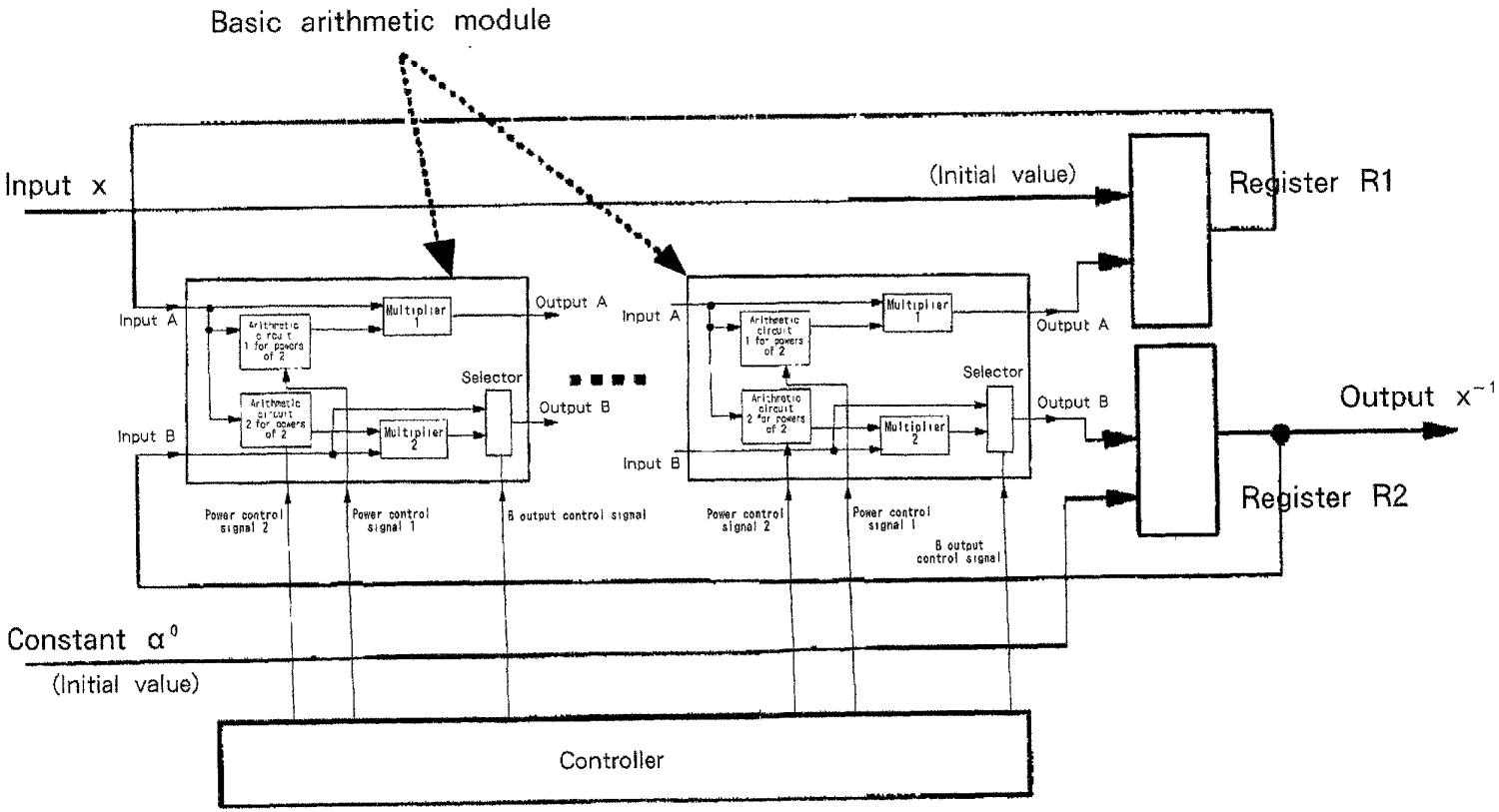
Multiplication device used for the circuit configuration

Fig. 4



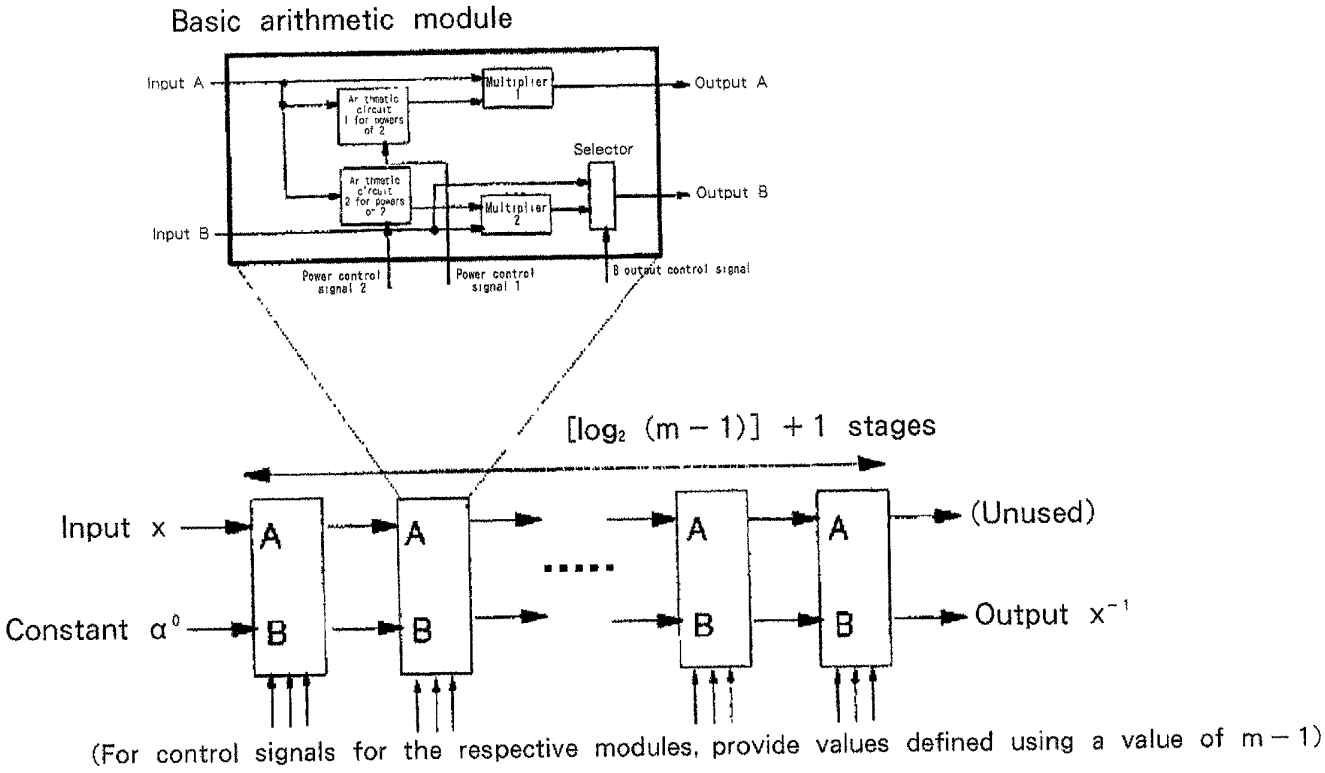
Overall configuration method 1 when a basic arithmetic module is provided as a sequential circuit

Fig. 5



Overall configuration method 2 when a basic arithmetic module is provided as a sequential circuit

Fig. 6



(For control signals for the respective modules, provide values defined using a value of m – 1)

Overall configuration method when a basic arithmetic module is provided as a combinational circuit

Fig. 7

1. Case wherein a sequential circuit is implemented :

Repeat the following $[\log_2 (m-1)]$ times
At the k – th cycle (k is a natural number),
the power arithmetic circuit 1 calculates 2^{k-1} powers of 2,
the power arithmetic circuit 2 calculates $\{(m-1) \bmod (2^{k-1})\} + 1$ powers of 2.
The output of the multiplier 1 is selected as the input for the register R1.
When in the binary expression m – 1 bit k – 1 is 1,
the output of the multiplier 2 is selected as the input for the register 2, and
in other cases,
the output of the register R2 is selected as the input of the register R2.

---

2. In a case where a combinational circuit is implemented :

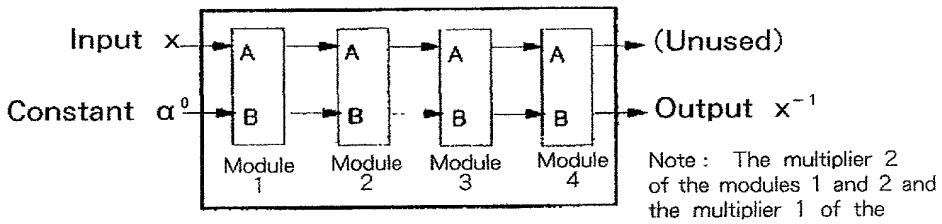
Modules 1, 2, 3, ... are defined from the input side to the output side, and the control signals for module k permit
the power arithmetic circuit 1 to calculate 2^{k-1} powers of 2, and
the power arithmetic circuit 2 to calculate $\{(m-1) \bmod (2^{k-1})\} + 1$ powers of 2.
When bit k – 1 is 1 in the binary expression,
the output of the multiplier 2 is selected as the output B,
while in other cases
the input B is selected as the output B.

When the combinational circuit is implemented, the multiplier that always receives the constant α° at one of the input terminals is deleted, and the other input terminal is connected to the output terminal of the multiplier.

Specific method for generating control signals for each module

Fig. 8

Multiplicative inverse arithmetic circuit for which m = 15



Note : The multiplier 2 of the modules 1 and 2 and the multiplier 1 of the module 4 can be deleted

	Power control S1	Power control S2	Output B control S0
Module 1	2^1 powers	(Powers not required)	Input B
Module 2	2^2 powers	2^1 powers	Input B
Module 3	2^4 powers	2^3 powers	Multiplier 2 output
Module 4	(Powers not required)	2^7 powers	Multiplier 2 output

Specific example of control signals to be provided for modules (m = 15)

Fig. 9

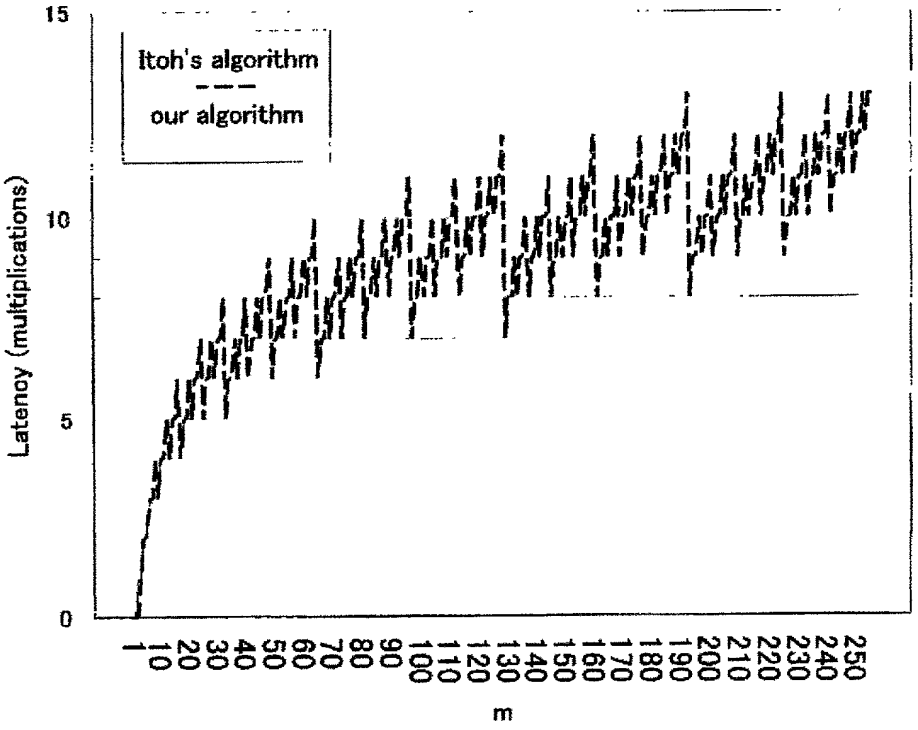


Fig. 10

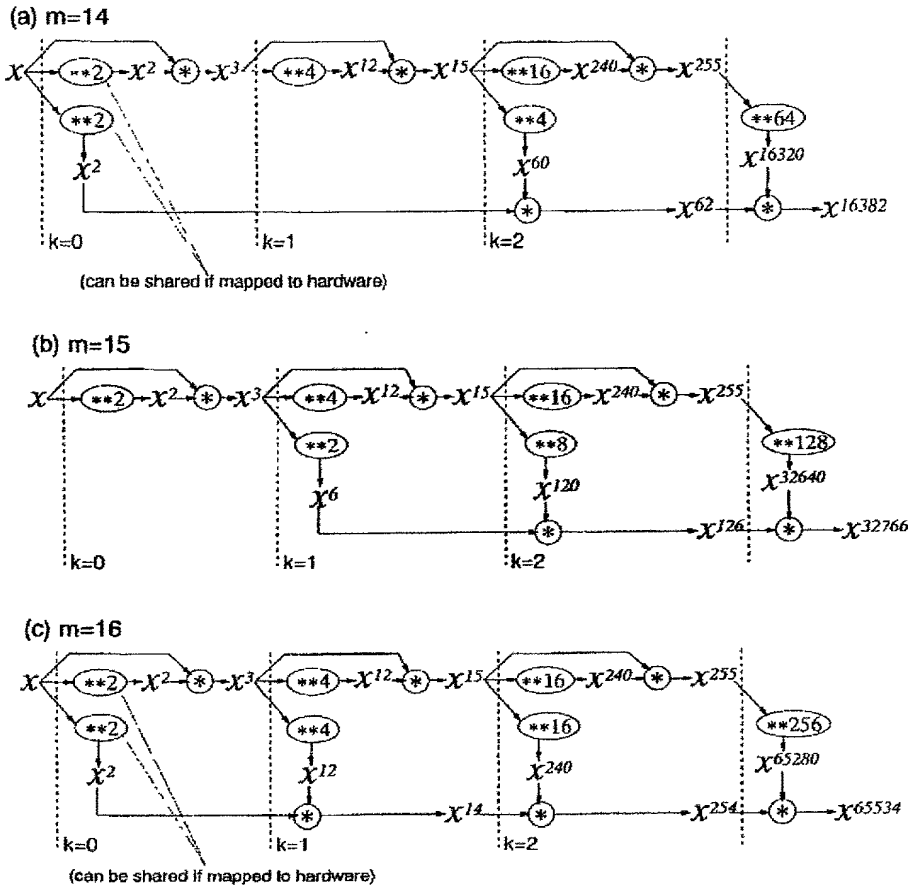

(a) m=14
k=0
k=1
k=2
(can be shared if mapped to hardware)
(b) m=15
k=0
k=1
k=2
(c) m=16
k=0
k=1
k=2
(can be shared if mapped to hardware)

Fig. 11

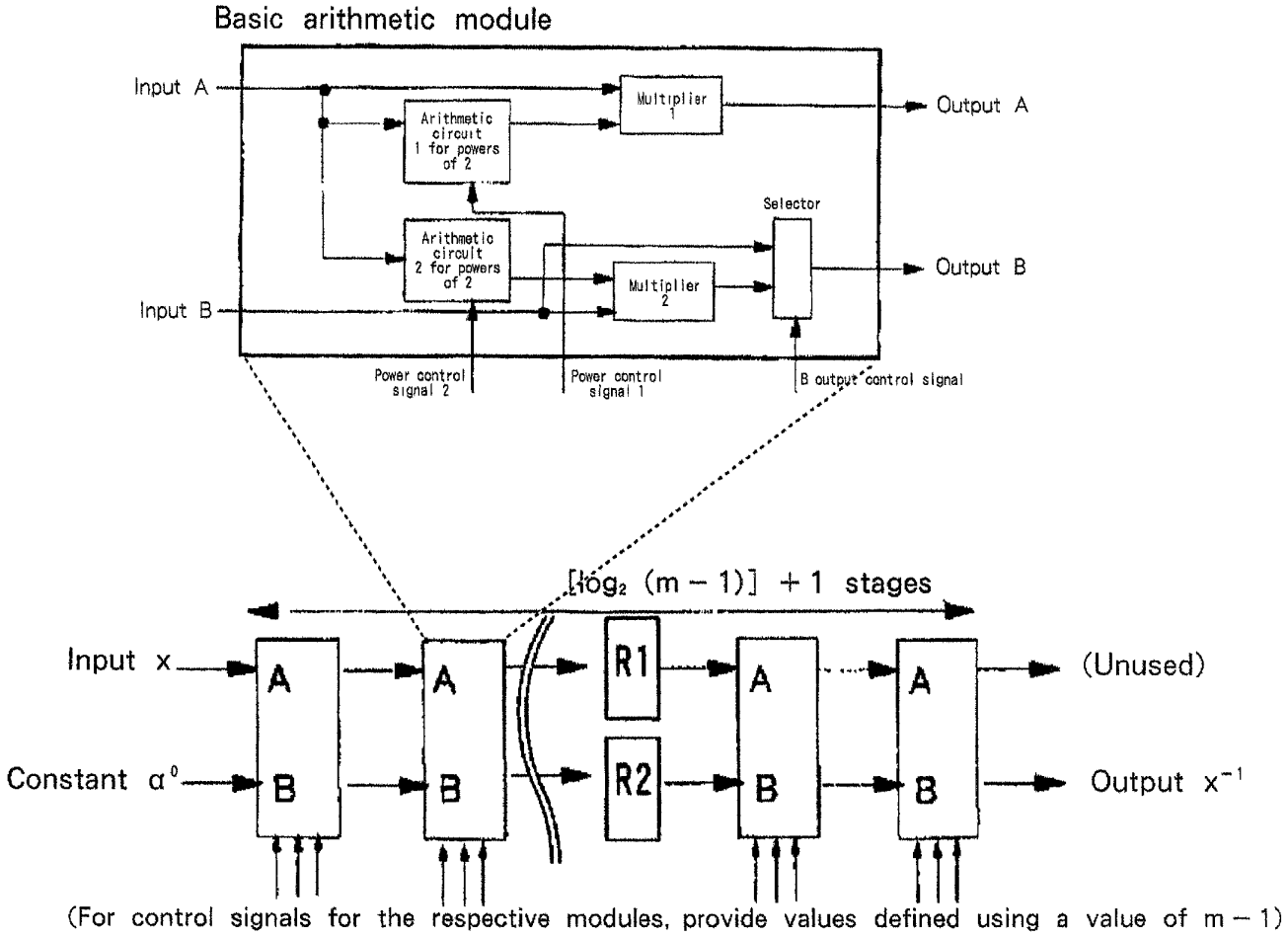

Basic arithmetic module
Input A
Input B
Arithmetic circuit 1 for powers of 2
Arithmetic circuit 2 for powers of 2
Multiplier 1
Multiplier 2
Selector
Output A
Output B
Power control signal 2
Power control signal 1
B output control signal
[log2 (m - 1)] + 1 stages
Input x
Constant α^0
A
B
R1
R2
(Unused)
Output x^-1
(For control signals for the respective modules, provide values defined using a value of m - 1)

Fig. 12